PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215590

(43)Date of publication of application : 02.08.2002

(51)Int.Cl. G06F 15/00
G06F 1/00
G06K 17/00
G06K 19/10
H04L 9/32

(21)Application number : 2001-009771

(22)Date of filing : 18.01.2001

(71)Applicant : TDK CORP

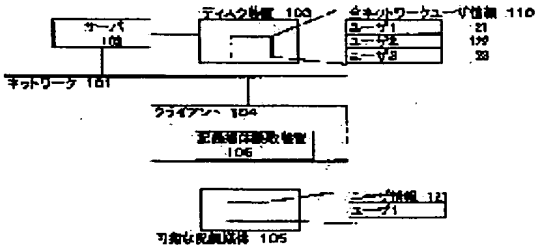
(72)Inventor : TSUNEKAWA HARUKI

(54) RECORDING MEDIUM FOR NETWORK LOG-IN AND NETWORK LOG-IN METHOD USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network log-in method which is convenient and protected against illegal use by using a portable recording medium for network log-in.

SOLUTION: User information is divided and recorded on a plurality of portable recording media for network log-in. Log-in operation is done by using the portable recording media and user information is ciphered to attain protection against illegal use. The user information is rewritten to the portable recording media at log-out time to make the security to the illegal use higher.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－215590
（P2002－215590A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｇ　５Ｂ０３５
	1/00	３７０		1/00	３７０Ｅ　５Ｂ０５８
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｔ　５Ｂ０８５
	19/10			19/00	Ｒ　５Ｊ１０４
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｃ

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願2001－9771(P2001－9771)

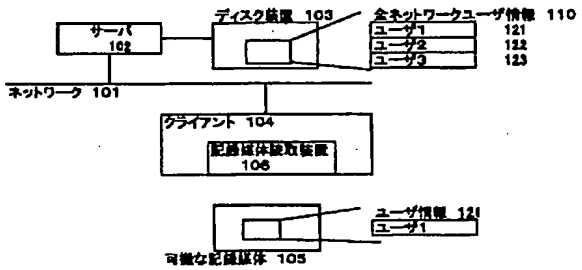
(22)出願日　平成13年１月18日(2001.1.18)

(71)出願人　000003067
ティーディーケイ株式会社
東京都中央区日本橋１丁目13番１号
(72)発明者　常川　春樹
東京都中央区日本橋一丁目13番１号　ティーディーケイ株式会社内

Ｆターム(参考)　5B035 AA14 BB09 BC01 CA38
5B058 CA27 KA02 KA04 KA08 KA31
KA35 YA20
5B085 AE02 AE11 AE29
5J104 AA07 AA12 AA16 EA03 EA13
KA01 NA02 NA05 NA27 NA30
NA36 PA07

(54)【発明の名称】　ネットワークログイン用記録媒体及びそれを用いるネットワークログイン方法

(57)【要約】　（修正有）
【課題】ネットワークログイン用の可搬な記録媒体を用いて簡便でかつ不正使用から保護されたネットワークログインの方法を提供する。
【解決手段】ネットワークログイン用の複数の可搬な記録媒体にユーザ情報を分割して記録しておく。この複数の可搬な記録媒体によりログインを行うとともに、ユーザ情報を暗号化することにより不正使用から保護する。またログアウトするときに当該ユーザ情報を当該可搬な記録媒体上に書き換えることにより不正使用に対する安全性をより一層高める。



1

【特許請求の範囲】

【請求項1】ネットワークログインするに必要なユーザ情報が分割して記録されていることを特徴とする複数枚の可搬な記録媒体。

【請求項2】上記可搬な記録媒体上に記録された上記ユーザ情報は公開鍵暗号方式で暗号化されていることを特徴とする、請求項１記載の記録媒体。

【請求項3】上記ユーザ情報はログアウトするときに上記ユーザ情報を書き換えることができることを特徴とする、請求項１又は請求項２に記載の記録媒体。

【請求項4】請求項１乃至3記載の記録媒体によりネットワークに接続するネットワークログイン方法

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ネットワークにログインする際に使用する記録媒体及びログイン方法に関する。

【０００２】

【従来の技術】ネットワークにログインするには、ログインするユーザはあらかじめ登録しておいたパスワードを用いて、キーボードより入力される正しいパスワードによって正しいユーザーとして認証され、ネットワークにログインするのが通常の方法である。しかしながら、ログインするごとにパスワードをキーボードから入力するのはユーザの利便性に欠ける。またパスワードを忘れてしまって正しいユーザであるにもかかわらず、ログインできない、あるいは、他人にパスワードを盗まれて不正にログインされてしまう、等の問題があった。そこで特開平３－２６８０５０号公報、特開平６－３４８６５０号公報に記載のように、ユーザ情報、パスワードなどからなるログイン情報を可搬な記録媒体上に記録しておき、該可搬な記録媒体を用いてログインする方法が考えられていた。

【０００３】

【発明が解決しようとする課題】上記のような可搬な記録媒体を用いてネットワークにログインする手段だけでは、可搬な記録媒体を使用するがためにこの記録媒体を不正に入手した者による不正なログインを完全に防止をすることはできなかった。

【０００４】

【課題を解決するための手段】上記のような課題を解決するため、本発明では可搬な記録媒体をもちいてネットワークにログインする手段としての該可搬な記録媒体を複数枚とすること、該記録媒体に記録する情報は公開鍵暗号方式で暗号化されていること、該情報はログアウトする毎に該可搬な記録媒体に再記録されることにより常に最新の情報に保たれること、などにより上記可搬な記録媒体を第三者が入手して不正にログインすることを防止できる手段を提供するものである。

【０００５】

2

【作用】可搬な記録媒体を用いてネットワークに自動的にログインする手段により、ネットワークの１クライアントPCからネットワークにアクセスするとともに、該可搬な記録媒体の不正使用を防止する。

【０００６】

【実施例】本発明の１実施例について図１を用いて説明する。

【０００７】図１を用いて、可搬な記録媒体上にあるユーザのログイン情報をもとに、ネットワークへ自動的にアクセスを開始する（以後これをログインと呼ぶ）原理を説明する。

【０００８】１０１はネットワーク、１０２はネットワーク（１０１）のサーバ、１０３はサーバ（１０２）に接続されているディスク装置、１０４はネットワーク（１０１）のクライアントPC、１０５はクライアントPCにより情報を読み書き可能な可搬な記録媒体、１０６はクライアントPC（１０４）に接続されている記録媒体読取装置である。本実施例では説明簡略化のため、サーバ（１０２）,クライアントPC（１０４）は各１つとなっているが、これらはネットワーク（１０１）上に複数あってもかまわない。

【０００９】ディスク装置（１０３）に保管されている、該サーバ（１０２）を用いている全ネットワークユーザ情報、１２１は可搬な記録媒体（１０５）内にある、ユーザ情報である。

【００１０】さらに、全ネットワークユーザ情報（１１０）にはネットワークユーザとしてユーザ１（１２１）、ユーザ2（１２２）、ユーザ３（１２３）に関するユーザ情報が記録されており、可搬な記録媒体（１０５）内にはユーザ１（１２１）一人分のログイン情報が記録されている。このような構成をもつネットワーク（１０１）において、ネットワークユーザであるユーザ１（１２１）が、自身のログイン情報が記録されている可搬な記録媒体（１０５）を、ネットワーク（１０１）上のクライアントPC（１０４）内にある記録媒体読取装置（１０６）に装着すると、クライアントPC（１０４）は可搬な記録媒体（１０５）内のユーザ情報（１２１）を読み、ログイン情報をサーバ（１０２）に送る。サーバ（１０２）は接続されているディスク装置（１０３）内にある全ネットワークユーザ情報（１１０）と照合してこのログイン情報が正しければ、ユーザ１（１２１）を認証して、ネットワーク（１０１）を利用することを許可する。もしも、前記ユーザ情報（１２１）と全ネットワークユーザ情報（１１０）との照合が正しくなければ、ユーザ１（１２１）は認証されずネットワーク（１０１）にログインできないためネットワークの利用をすることはできない。

【００１１】図１では便宜上可搬な記録媒体にユーザ情報すべてを記録してあるものとして説明したが、本発明はユーザ情報が複数枚の記録媒体に分割されていること

に特徴がある。以下、図２及び図３を用いてこれを説明する。

【００１２】ユーザ情報（１２１）は図２に示すように、ユーザの名前、ＩＤ番号、パスワード、ユーザのアクセスレベル、ユーザとして許される期限、などから構成される。このユーザ情報（１２１）を図１では可搬な記録媒体（１０５）のなかに一括して記録してあるものとして説明したが、一部づつ複数の媒体に分ける。ここでは可搬な媒体を2枚用いる例を図３により説明する。ユーザ情報（１２１）は２枚の可搬な媒体（１０５ａと１０５ｂ）のなかにユーザ情報ａ（１２１ａ）とユーザ情報ｂ（１２１ｂ）とに分かれて記録されている。まず第一の可搬な媒体（１０５ａ）を図１と同様にクライアントPC（１０４）に接続されている記録媒体読取装置（１０６）に装着するとクライアントPC（１０４）は可搬な記録媒体（１０５ａ）内のユーザ情報の一部（１２１ａ）を読む。クライアントPC（１０４）はサーバ（１０２）に読み取ったユーザ情報（１２１ａ）を送る。サーバ（１０２）は全ネットワークユーザ情報（１１０）中のユーザ情報（１２１から１２３）を調べるがユーザ情報の一部（１２１ａ）しかないためユーザ情報（１２１）を構成できずログインが許可されないことをクライアントPCに伝える。ここでユーザはもう一枚の可搬な記録媒体（１０５ｂ）をクライアントPC（１０４）に接続された記録媒体読取装置（１０６）に装着すると、クライアントPC（１０４）は可搬な記録媒体（１０５ｂ）よりユーザ情報の残りの部分（１２１ｂ）を読む。クライアントPC（１０４）はサーバ（１０２）に２枚目の可搬な記録媒体（１０５ｂ）から読み取ったユーザ情報（１２１ｂ）を送る。サーバ（１０２）は全ネットワークユーザ情報（１１０）中のユーザ情報（１２１から１２３）を調べ、全てのユーザ情報（１２１）が構成されていることを知るのでログインを許可する。

【００１３】このようにしてログイン情報を２枚の可搬な記録媒体に分割して記録することにより悪意ある第三者がこの可搬な記録媒体を不正に入手しようとしても２枚を入手する必要があり、１枚のときよりも著しく不正に使用される危険が減少していることは言うまでもない。また３枚以上に分割すれば不正に使用される危険はより減少する。

【００１４】ユーザ情報（１２１）の分割の方法としてユーザ情報（１２１）の構成要素である　ユーザの名前、ＩＤ番号、パスワード、ユーザのアクセスレベル、ユーザとして許される期限、などの項目を分割して記録してもいいし、パスワードの上位桁、下位桁のように項目内で分割して記録しても効果は同じように期待される。

【００１５】図４を用いてユーザ情報の暗号化について説明する。

【００１６】悪意ある第三者がユーザ情報（１２１）の記録された可搬な記録媒体を不正に入手し、ユーザ情報（１２１）を改ざんして使用することがある。例えばより機密性の高い情報にアクセス可能となるべく、ユーザアクセスレベルを通常レベルからより高い管理者レベルに改ざんしたり、アクセス可能期限がきれているにもかかわらず、期限情報を改ざんしてアクセスを可能としたりする場合が予想される。改ざんを防止するには、上記可搬な記録媒体内のユーザ情報（１２１）を容易に読むことができないように、暗号化を施せばよい。ただし、通常の暗号化では、暗号化のための「鍵」をサーバ（１０２）とクライアントPC（１０４）が共有するため、「鍵」の秘匿管理を十分行う必要がある。ましてネットワーク上のように多くの人に公開された場であると「鍵」をネットワークでサーバ（１０２）とクライアントPC（１０４）の間で送受するときに、傍受されてしまう危険性もある。

【００１７】そこで、この暗号化の手法として「公開鍵暗号方式」をもちいてユーザ情報（１２１）を暗号化しておけばよい。「公開鍵暗号方式」としてはRSA方式が著名である。ＲＳＡ暗号方式については、例えば文献「情報セキュリティの科学」ＢＬＵＥＢＡＣＫＳ　Ｐ１３０～に述べられている。最初にサーバ（１０２）はクライアントPC（１０４）との間にRSA方式による「秘密鍵」（１４１）「公開鍵」（１４２）を定め、クライアントPC(１０４)には「公開鍵」を提示する。クライアントPCはこの「公開鍵」を用いて、ユーザ情報（１２１）を暗号化する。クライアントPC（１０４）はこの暗号化されたユーザ情報（１２１Ｅ）をサーバ（１０２）に送る。サーバ（１０２）は「秘密鍵」により暗号化されたユーザ情報（１２１Ｅ）を解き、全ネットワークユーザ情報（１１０）と比較して、ログインの可否を決める。

【００１８】図５を用いてログアウトするとき上記可搬な記録媒体上にユーザ情報（１２１）を書き換えることについて説明する。なお、ログアウトとはユーザがネットワークからの接続を切って離れることをいう。

【００１９】上記「公開鍵暗号方式」にて暗号化されたユーザ情報であるが、悪意ある第三者からの情報保護のうえでは、暗号の鍵を時々更新するのが望ましい。本発明ではこれをログアウトするときに更新し、ユーザ情報（１２１）の保護を図っている。ユーザがログアウトするときは、サーバ（１０２）は新たな「秘密鍵」と「公開鍵」を作成する。

【００２０】サーバ（１０２）は接続されているディスク装置（１０３）に保管されている全ネットワークユーザ情報（１１０）より、当該ログアウトするユーザ情報（ここではユーザ１を例として説明する）（１２１）を取り出し、ネットワーク（１０１）を経由してクライアントPC（１０４）に送る。このときサーバ（１０２）は新たに作成した「公開鍵」（１４２）もクライアントPC（１０４）に送る。クライアントPCはこのユーザ情報

5

（１２１）を当該「公開鍵」（１４２）にて暗号化し、クライアントPCに接続されている記録媒体書込み装置（１０７）に挿着された可搬な記録媒体（１０５）に暗号化されたユーザ情報（１２１ｅ）として記録する。

【００２１】

【発明の効果】可搬な媒体を用いてログインするため正規ユーザにはキー入力時の負担を減らすことができ、さらに暗号化された複数の媒体を用いることによる、第三者の不正なログインを防止することができる。

【図面の簡単な説明】

【図１】可搬な記録媒体上のユーザ情報を用いてネットワークにログインする原理図である。

【図２】ユーザ情報の内容の例を示す図である。

【図３】ユーザ情報が分かれて記録された複数の可搬な記録媒体の図である。

6

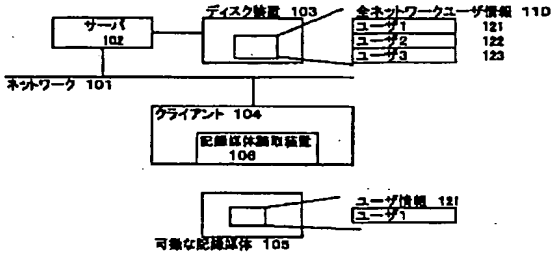
＊【図４】ユーザ情報の暗号化を行う原理図である。

【図５】ユーザ情報をログアウト時に可搬な記録媒体に書き込む原理図である。

【符号の説明】

１０１…ネットワーク、１０２…サーバ、１０３…ディスク装置、１０４…クライアントPC、１０５…可搬な記録媒体、１０５ａ…第一の可搬な記録媒体、１０５ｂ…第二の可搬な記録媒体、１０６…記録媒体読取装置、１０７…記録媒体書込装置、１１０…全ネットワークユーザ情報、１２１…ユーザ情報、１２１ａ…第一の可搬な記録媒体に記録されている一部のユーザ情報、１２１ｂ…第二の可搬な記録媒体に記録されている一部のユーザ情報、１２１ｅ…暗号化されたユーザ情報、１２１から１２３…各ユーザ情報、１４１…暗号化のための秘密鍵、１４２…暗号化のための公開鍵

【図１】

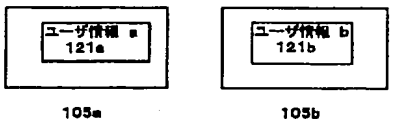


【図２】

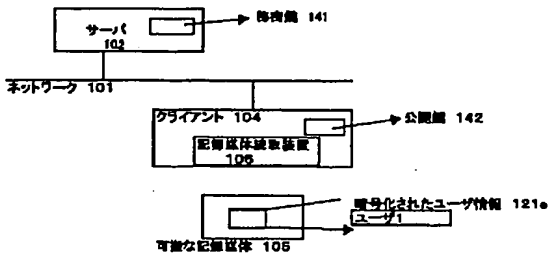
ユーザ情報 121

ユーザ名	ユーザ1
ID	ABCD
パスワード	1234
ユーザアクセスレベル	通常
期限	2001/12/31
その他の情報	なし

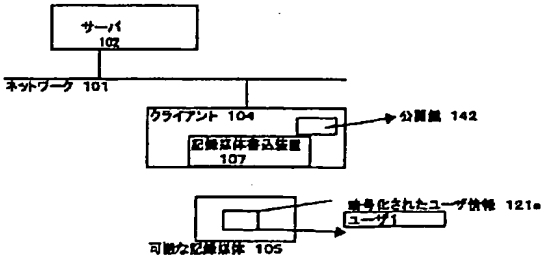
【図３】



【図４】



【図５】



フロントページの続き

(51)Int.Cl.'	識別記号	FI	テーマコード' (参考)
		H04L 9/00	673E